

PATENT ABSTRACTS OF JAPAN

(11)Publication number : 01-163871

(43)Date of publication of application : 28.06.1989

(51)Int. Cl.

G06F 15/21

G06F 15/22

H04L 9/00

H04L 23/00

(21)Application number : 62-321220

(71)Applicant : HITACHI LTD

(22)Date of filing : 21.12.1987

(72)Inventor : GOTOU YASUKO
TAKARAGI KAZUO
SASAKI RYOICHI

(54) HIERARCHIZATION SYSTEM FOR SLIP COMPRESSED SENTENCE

(57)Abstract:

PURPOSE: To smooth an electronic transaction through an information network by enabling a slip confirmation by a segment-wise compressed sentence by the completion stage of a transaction, enabling to detect the falsification of a slip and enabling a unique digital signature reflecting a slip content.

CONSTITUTION: An electronic transaction is executed between computers 101 and 102 connected by a network 103. A slip prepared here is divided into some segments, data to be the point of a transaction are included in each divided segment, a compressed sentence is prepared for each segment, a compressed sentence including the content of the compressed sentence for each segment is prepared and it turns to be a representative compressed sentence in a transaction slip. The representative compressed sentence is used for a digital signature in the electronic transaction and the compressed sentences of each segment are preserved for the false detection of a slip falsification and the like. Thus, such electronic transaction such as the signing and sealing of contracts with the use of a computer can be attained.



LEGAL STATUS

[Date of request for examination]

[Date of sending the examiner's decision of rejection]

[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]

[Date of final disposal for application]

[Patent number]

[Date of registration]

[Number of appeal against examiner's decision of rejection]

[Date of requesting appeal against examiner's decision of rejection]

[Date of extinction of right]

⑨ 日本国特許庁(JP)

⑩ 特許出願公開

⑫ 公開特許公報(A) 平1-163871

⑬ Int. Cl.⁴

G 06 F 15/21
15/22
H 04 L 9/00
23/00

識別記号

庁内整理番号

Z-7230-5B
7230-5B
A-7240-5K
A-7240-5K

⑭ 公開 平成1年(1989)6月28日

審査請求 未請求 発明の数 1 (全4頁)

⑮ 発明の名称 伝票圧縮文階層化方式

⑯ 特 願 昭62-321220

⑰ 出 願 昭62(1987)12月21日

⑱ 発 明 者 後 藤 寧 子 神奈川県川崎市麻生区王禅寺1099番地 株式会社日立製作所システム開発研究所内

⑲ 発 明 者 宝 木 和 夫 神奈川県川崎市麻生区王禅寺1099番地 株式会社日立製作所システム開発研究所内

⑳ 発 明 者 佐々木 良一 神奈川県川崎市麻生区王禅寺1099番地 株式会社日立製作所システム開発研究所内

㉑ 出 願 人 株式会社日立製作所 東京都千代田区神田駿河台4丁目6番地

㉒ 代 理 人 弁理士 小川 勝男 外1名

明 細 書

1. 発明の名称

伝票圧縮文階層化方式

2. 特許請求の範囲

1. 電子取引において、相手認証、および取引内容(伝票)の確認を行なうために用いる取引者同士が必要とする伝票の圧縮文作成において、該伝票の全部あるいは一部をいくつかに分割し、かつ分割した各部位には、取引伝票におけるポイントとなるデータを含め、該分割部位毎に、圧縮文を作成し、部位毎の該圧縮文から、該伝票内容を反映した一意的な代表圧縮文を作成し、該代表圧縮文を用いてデジタル署名を行うことにより、取引の終了段階までに、部位別圧縮文による伝票確認を可能とするとともに、伝票の不正改ざん検知を可能とし、さらに伝票内容を反映した一意的なデジタル署名を可能とすることを特徴とする伝票圧縮文階層化方式。

3. 発明の詳細な説明

(産業上の利用分野)

本発明は、情報ネットワークを介した電子取引に関する。

(従来の技術)

いま、通信ネットワークを介して、会議や種々の取引を電子的に行うビジネス通信の時代が始まろうとしている。近い将来、コンピュータを用いて契約書に署名、捺印するといった電子取引も実現するものと予想される。

公例鍵暗号を応用して作成されるデジタル署名は、電子取引において次の機能をもたらすものとして注目されている。

(1) 送信者は、通信事実、および通信内容を否定することができない。

(2) 受信者は、通信事実、および通信内容を否定することができない。

これにより、デジタル署名は従来の印鑑に相当する機能をデータ通信において実現し得るものと期待されている。

(発明が解決しようとする課題)

ところで、電子取引におけるデジタル署名は

取引伝票の圧縮文と取引状況を示す内容とから成り、取引伝票の圧縮文は、取引伝票の内容が1ビットでも異なれば全く別のものになるという極めて感度の高いものである。

従つて、不当に取引伝票を改ざんされた場合、本来できるべき圧縮文を改ざんされた伝票の圧縮文が異なり、伝票改ざんを証明することになる。

しかしながら、伝票を改ざんした事実を証明することは可能でも、伝票におけるどの部位を改ざんしたかを証明することは不可能であつた。

〔問題点を解決するための手段〕

上記の問題点を解決するために、本発明では次の手段を用いる。

- (1) 作成する伝票をいくつかに分割する。分割した各部位には、取引のポイントとなるようなデータを含ませる。
- (2) 各部位毎に圧縮文を作成し、各部位毎の圧縮文の内容を含む圧縮文を作成し、これを取引伝票における代表圧縮文とする。
- (3) 電子取引におけるデジタル署名には、代表

により、デジタル署名は、伝票内容を反映した一意的なものとして実現することも可能である。〔実施例〕

以下、本発明の一実施例を、第1図、第2図により説明する。第1図に示すネットワークで結ばれた二者間において電子取引を行う。

step1: 計算機101、あるいは102において、取引伝票201は、所定の規約に基づき、M1(202)、M2(203)、M3(204)、M4(205)の4部位(ここでは4部位とする)に分割する。

M1の部位データには、銘柄データを含ませ、

M2の部位データには、売買データを含ませ、

M3の部位データには、株数データを含ませ、

M4の部位データには、指値データを含ませる。

step2: 分割した部位データM1~M4について、各々のデータから部位圧縮文MAC1~MAC4を計算機101(あるいは102)上で作成する。圧縮文作成方式については後述する。

step3: 部位圧縮文MAC1~MAC4を基に、

圧縮文を用い、各部位の圧縮文は、伝票改ざん等の不正検知用として保存する。

〔作用〕

前記技術的手段により、次の作用が生じる。

1. 不注意なミスによる不要な取引の減少

取引において、遅けがたいヒューマン・エラーに対し、取引段階で各部位ごとの圧縮文作成及び圧縮文のチェックを行うことにより、ヒューマン・エラーを検知することができ、不必要な取引を行うことを避けることが容易になる。

2. 取引伝票の不正な改ざん部位を検知

分割した伝票の各部位に、取引のポイントとなるデータ(例えば、株式売買においては、指値、株数、銘柄、売買等)を含ませることにより各部位毎における各部位圧縮文は、各ポイントデータを反映するものと考えられるので、改ざん部位を推定することが容易になる。

3. 伝票内容を反映したデジタル署名

部位圧縮文全てを入力データとして作成した代表圧縮文をデジタル署名の原文とすること

取引伝票201の代表圧縮文MACを計算機101(あるいは102)において、作成し、MACおよびMAC1~MAC4を伝票201の圧縮文データとする。

step4: 計算機101(計算機102)において、作成して圧縮文と伝票データを通信ネットワーク103を介して、計算機102(計算機101)に送信し、以下電子取引(電子捺印交換)を行う。

step5: 計算機102(計算機101)では、同様に部位圧縮文と代表圧縮文を作成し、取引伝票のチェックを行う。ここで、不注意な伝票作成ミス等の検知を行う。

step6: 計算機102(あるいは101)において、電子捺印交換を行う際、代表圧縮文を用いてデジタル署名を行い、電子取引を行う。

step7: 取引後、計算機101と102間において、くい違いが生じた場合、主張する伝票の部位圧縮文、および、代表圧縮文を作成し、比較することにより、伝票データの不正な改ざん検知と改ざん部位の推定を行う。

圧縮文作成は、取引伝票Mを56ビット長のブロックに区切り、各ブロックをM1, M2, … Mnとする。最後のMnが56ビット長に満たない時は、“0”を付加し、補正する。

前記ブロックに対し、7ビット単位で1ビットのパリティ・ビットを付加し、ブロック長を64ビットに拡張し、これをK1, K2…Knとする。

入力データI(i-1)を鍵Kiで暗号化(E)したものとI(i-1)との排他的論理和をとつたものをI(i)とする。

$$I(i) = I(i-1) \oplus EK_i(I(i-1))$$

以上の処理を、i=1, 2…について行う。また、初期値I(0)は、予め定められた値とする。ただし \oplus は、ビット対応の排他的論理和を表す。

最終的に求められた値I(n)が圧縮文となる。

前記部位圧縮文は、取引伝票Mの一部から作成するものである。

実施例の変形例1

伝票の分割方法は必要と要求に応じて、均等分

割、レベル別分割、あるいは、わりふり分割等を行うことも可能である。また分割は、伝票全体、あるいは一部に対して行うことも可能である。

実施例の変形例2

部位圧縮文は、部位毎に独立のものとするのも、あるいは、部位M1の圧縮結果を部位M2が包括し、部位M3は部位M2の圧縮結果を包括するものとするのも可能である。

【発明の効果】

1. 不注意なミスによる不要な取引の減少、

取引において、避けがたいヒューマン・エラーに対し、取引段階で各部位毎の圧縮文作成、及び部位圧縮文のチェックを行うことにより、ヒューマン・エラーを検知することができ、不必要な取引を行うことを避ける。

2. 伝票改ざん部位を検知

分割した伝票の各部位に、取引のポイントとなるゲータ（例えば、株式売買においては、指値、株数、銘柄、売買等）を含ませることにより、各部位毎における部位圧縮文は、各ポイン

トデータを反映するものと考えられるので、改ざん部位を指定することが容易にできる。

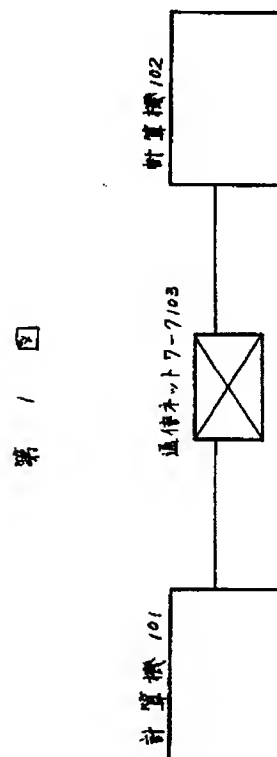
3. 伝票内容を反映したデジタル署名

各部位圧縮文を入力データとして作成した代表圧縮文をデジタル署名の原文とすることにより、デジタル署名は、伝票内容を反映した一定的なものとして実現することも可能である。

4. 図面の簡単な説明

第1図は本発明を実施する電子取引システムの構成例を示すブロック図、第2図は本発明の電子取引における伝票の階層的圧縮文作成のための、株式売買を想定した伝票の分割例を示す説明図である。

代理人 弁護士 小川勝男



第 2 図

郵便M1:202 郵便M2:203 郵便M3:204 郵便M4:205

株式会社 東京注文伝書

郵便	郵便	郵便	郵便	郵便
日東航空	買	1200	1000	
住所	(〒661) Tel. (04-621-2098)			
	横浜市中区山中 4-5-6			
氏名	山田桃太郎			
電子捺印				
約定時刻				
野山証券(株)	取扱: 梅生営業所			
	(〒123) Tel. (044-966-6421)			
	川崎市王様寺町 1-2-3			
電子捺印				

伝書201